TOLER SCHAFFER LLP
8500 Bluffstone Cove, Suite A201
Austin, Texas 78759
Phone 512-327-5515
Fax 512-327-5575

FACSIMILE COVER SHEET

DATE: October 4, 2007

TO: Examiner HOANG, Daniel L. **FAX NO.:** 571-273-8300
USPTO GPAU 2136

FROM: Jeffrey G. Toler
Reg. No.: 38,342

RE U.S. App. No.: 10/634,117, filed August 4, 2003

Applicant(s): James M. Doherty, et al.

Atty Dkt No.: 1033-T00534

Title: HOST INTRUSION DETECTION AND ISOLATION

NO. OF PAGES (including Cover Sheet): 10

MESSAGE:

Attached please find:

☒ Transmittal Form (1 pg)
☒ Reply Brief (8 pgs)

8500 Bluffstone Cove
Suite A201
AUSTIN, TEXAS 78759

Tel: (512) 327-5515
Fax: (512) 327-5575

RECEIVED
CENTRAL FAX CENTER
OCT 0 4 2007

PTO/SB/21 (04-07)
Approved for use through 09/30/2007. OMB 0851-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission: 10

Application Number	10/634,117
Filing Date	August 4, 2003
First Named Inventor	James M. Doherty, et al.
Art Unit	2136
Examiner Name	HOANG, Daniel L.
Attorney Docket Number	1033-T00534

ENCLOSURES *(Check all that apply)*

- ☐ Fee Transmittal Form
  - ☐ Fee Attached
- ☐ Amendment/Reply
  - ☐ After Final
  - ☐ Affidavits/declaration(s)
- ☐ Extension of Time Request
- ☐ Express Abandonment Request
- ☐ Information Disclosure Statement
- ☐ Certified Copy of Priority Document(s)
- ☐ Reply to Missing Parts/ Incomplete Application
  - ☐ Reply to Missing Parts under 37 CFR 1.52 or 1.53
- ☐ Drawing(s)
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert to a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s) _____
  - ☐ Landscape Table on CD
- ☐ After Allowance Communication to TC
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☑ Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- ☐ Proprietary Information
- ☐ Status Letter
- ☐ Other Enclosure(s) (please identify below):

Remarks

Customer No.: 60533

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	Toler Schaffer LLP		
Signature			
Printed name	Jeffrey G. Toler		
Date	10-4-2007	Reg. No.	38,342

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature			
Typed or printed name	Jeaneaux Jordan	Date	10-4-07

Attorney Docket No.: 1033-T00534

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s):	**James M. Doherty, et al.**		
Title:	**HOST INTRUSION DETECTION AND ISOLATION**		
App. No.:	**10/634,117**	Filed:	**August 4, 2003**
Examiner:	**HOANG, Daniel L.**	Group Art Unit:	**2136**
Customer No.:	**60533**	Confirmation No.:	**5753**
Atty. Dkt. No.:	**1033-T00534**		

BOARD OF PATENT APPEALS
AND INTERFERENCES
United States Patent
and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

REPLY BRIEF

Jeffrey G. Toler, Reg. No. 38,342
Attorney for Applicants
TOLER SCHAFFER, LLP
8500 Bluffstone Cove, Suite A201
Austin, Texas 78759
(512) 327-5515 (phone)
(512) 327-5575 (fax)

I. STATUS OF CLAIMS (37 C.F.R. § 41.37(c)(1)(iii))

A. Total Number of Claims in Application

There are 25 claims pending in the application (claims 1, 3-15, and 17-27).

B. Status of All the Claims

Claims 1, 14, and 15 are independent claims. According to pages 2-7 of the Final Office Action dated October 18, 2006 and according to pages 3-10 of the Examiner's Answer, which was mailed on August 17, 2007, the Examiner states that claims 1, 3-15, and 17-27 stand rejected, and are appealed. Claims 2 and 16 were canceled in the Amendment filed September 12, 2006.

C. Claims on Appeal

There are 25 claims on appeal (claims 1, 3-15 and 17-27).

II. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL (37 C.F.R. § 41.37(c)(1)(vi))

Claims 1, 3-15 and 17-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Publication No. 2004/0049693 ("Douglas") in view of U.S. Patent No. 6,081,894 ("Mann").

III. ARGUMENT (37 C.F.R. § 41.37(c)(1)(vii))

Appellant respectfully appeals each of the rejections applied against all claims now pending on appeal.

CLAIMS 1 and 3-13 ARE ALLOWABLE OVER DOUGLAS AND MANN

Appellant respectfully traverses the rejection of claims 1 and 3-13 under 35 U.S.C.§103(a) over U.S. Patent Publication No. 2004/0049693 ("Douglas") in view of U.S. Patent No. 6,081,894 ("Mann"), at page 3 of the Final Office Action and at pages 3-5 and 6-8 of the Examiner's Answer. The asserted combination of Douglas and Mann teaches away from independent claim 1.

The Final Office Action (pp. 3-4) and the Examiner's Answer (p. 3) acknowledges that Douglas does not disclose or suggest "in response to detecting the intrusion event, isolating the at least one network interface from the computer network and taking the host computer system down to a single user state so that access to the host computer system is limited to physical access at the host computer system," as recited by independent claim 1. The Office asserts that Mann discloses this element. *See Final Office Action*, p. 4 and the *Examiner's Answer*, p. 3.

The Examiner's Answer and the Final Office Action misconstrue the teachings of Mann. For example, citing Mann, the Examiner's Answer asserts that Mann discloses "taking the host computer system down to a single user state, as recited in claim 1. See Examiner's Answer, p. 3, citing Mann, col. 3, lines 2-5. However, the cited passage discloses a data isolator that is responsive to a data comparator to isolate a first data channel from a second data channel to prevent viruses from being received by a data receiving entity. *See Mann*, col. 3, lines 2-5. Mann does not teach "taking the host computer system down to a single user state," as recited in claim 1. Instead, Mann discloses that the operating state of the receiving data entity is not disrupted. Specifically, Mann discloses that a "further advantage of the invention is that it isolates the data sending entity from the data receiving entity without disrupting normal operation of either entity." See Mann, col. 2, lines 30-32 (emphasis added). Thus, Mann fails to disclose or suggest "taking the host computer down to a single user state," as recited in claim 1.

Thus, the asserted combination of Douglas and Mann fails to disclose or suggest each and every element of claim 1, and of claims 3-13, at least by virtue of their dependency from allowable claim 1.

CLAIMS 15 and 17-27 ARE ALLOWABLE OVER DOUGLAS AND MANN

Appellant respectfully traverses the rejection of claims 15 and 17-27 under 35 U.S.C.§103(a) over Douglas and Mann, at page 3 of the Final Office Action and at pages 3, 5-6 of the Examiner's Answer. The Final Office Action (*Final Office Action*, pp. 3-4) and the Examiner's Answer (p. 3) acknowledges that Douglas does not disclose or suggest, "in response to detecting an intrusion event, isolating at least one network interface from a computer network

and taking a host system down to a single user state so that access to the host computer system is limited to physical access at the host computer system," as recited by independent claim 15.

Claim 15 recites a system that includes "a host computer system having at least one network interface interfaced with a computer network," where the host computer system is to "operate in a multi-user mode," "detect an intrusion event using a system daemon," and "in response to detecting the intrusion event, isolate the at least one network interface from the computer network and take the host computer system down to a single user state so that access to the host computer system is limited to physical access at the host computer system."

Mann fails to disclose or suggest "taking the host computer down to a single user state," as recited in claim 15. In direct contrast to claim 15, Mann discloses that a "further advantage of the invention is that it isolates the data sending entity from the data receiving entity without disrupting normal operation of either entity." *See Mann*, col. 2, lines 30-32 (emphasis added). Hence, Mann fails to disclose or suggest "taking the host computer down to a single user state," as recited in claim 15.

Thus, the asserted combination of Douglas and Mann fails to disclose or suggest each and every element of claim 15, and of claims 17-27, at least by virtue of their dependency from allowable claim 15. For at least the foregoing reasons, the rejection of claims 15 and 17-27 over Douglas and Mann should be withdrawn.

CLAIM 14 IS ALLOWABLE OVER DOUGLAS AND MANN

Appellant respectfully traverses the rejection of claim 14 under 35 U.S.C. §103(a) over Douglas in view of Mann at pages 3 and 6 of the Final Office Action and at page 5 of the Examiner's Answer. None of the cited references, alone or in combination, recite the particular combination of independent claim 14.

The Final Office Action and the Examiner's Answer reject claim 14 over "Douglas and Mann as applied to claims 1-8 and 10." *See Final Office Action*, p. 6 and *see Examiner's Answer*, p. 5. However, both the Final Office Action and the Examiner's Answer fail to indicate

the particular bases for the rejection, and the Appellant is left to guess as to how the Office is interpreting the references to apply to the actual claim language.

Appellant notes that claim 14 recites:

A method comprising:
providing a host computer system having at least one network interface interfaced with a computer network;
operating the host computer system in a multi-user mode;
executing a system daemon on the host computer system;
reading, by the system daemon, a configuration file that indicates at least one file in a file system of the host computer system to be monitored for intrusion, wherein the configuration file comprises a first directive type that indicates a directory whose members are to be monitored for intrusion, a second directive type that indicates a file to be monitored for intrusion, and a third directive type that indicates another configuration file to be monitored for intrusion;
reading a valid MD5 signature for a monitored file from a database that is located on a second computer system isolated physically and programmatically from the host computer system;
detecting an intrusion event using the system daemon by detecting that an MD5 signature of the monitored file differs from the valid MD5 signature; and
in response to detecting the intrusion event:
issuing an IFCONFIG down command to the at least one network interface to isolate the at least one network interface from the computer network;
issuing an INIT1 command to an operating system of the host computer system to take the host computer system down to a single user state; and
writing a log of the intrusion event to a log database that is not located on the second computer system.

The cited references, alone or in combination, do not disclose or suggest the particular combination of claim 14. For example, the asserted combination of Douglas and Mann fails to disclose or suggest a method that includes "operating the host computer system in a multi-user mode" and, "in response to detecting the intrusion event," "issuing an INIT1 command to an operating system of the host computer system to take the host computer system down to a single user state," as recited in claim 14. As discussed above, Mann provides isolation "without disrupting normal operation of either entity" (i.e., without disrupting normal operation of a data sending entity or a data receiving entity). *See Mann*, col. 2, lines 30-32. Thus, Mann fails to teach or suggest issuing a command "to take the host computer system down to a single user

state," as recited in claim 14. Accordingly, claim 14 is allowable over the asserted combination of Douglas and Mann.

For at least the foregoing reasons, Appellant respectfully submits that the present application is in condition for allowance and reconsideration is respectfully requested.

RESPONSE TO EXAMINER'S ARGUMENT

The Examiner's Answer states that "the combination of the personal computer and the Internet is viewed as a system communicating in a multi-user state." *See Examiner's Answer*, p. 7. Appellant notes that the Office cites no support for this interpretation. Rejections on obviousness cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness. *See KSR Int'l Co. v. Teleflex Inc.*, citing *In re Kahn*, 441 F.3d 977, 988 (CA Fed. 2006). However, the factfinder must be aware of distortion caused by hindsight bias and must be cautious of arguments reliant upon ex post reasoning. *See KSR Int'l Co. v. Teleflex Inc.*, *citing Graham v. John Deere*, 383 U.S., at 36. "Determination of obviousness cannot be based on the hindsight combination of components selectively culled from the prior art to fit the parameters of the patented invention." *See ATD Corp. v. Lydall, Inc.*, 159 F.3d 534, 48 USPQ2d 1321 (Fed. Cir. 1998); *see also KSR Int'l Co. v. Teleflex Inc.*, 383 U.S., at 36.

The Examiner's Answer states "the combination of the personal computer and the Internet is viewed as a system communicating in multi-user state. The isolation of the computer from the Internet results in the computer operating in a single user state." *See Examiner's Answer*, p. 7. Appellant respectfully traverses the asserted interpretation. The asserted interpretation is unsupported by the cited references. Communications between a first user at a data sending entity and a second user at a data receiving entity does not implicate a user state of the data receiving entity.

Additionally, the cited references do not disclose or suggest that a multi-user mode is required for a personal computer to communicate with the Internet. Mann makes no mention of a multi-user mode. The Office interprets Mann as disclosing a multi-user mode by introducing a

system that includes the Internet (i.e., the data sending device) and the personal computer (i.e., the data receiving device), where "the combination of the personal computer and the Internet is viewed as a system communicating in a multi-user mode." *See the Examiner's Answer*, p. 7. In contrast to Mann, claim 1 recites:

> operating the host computer system in a multi-user mode;
> detecting an intrusion event using a system daemon; and
> in response to detecting the intrusion event, isolating the at least one network interface from the computer network and taking the host computer system down to a single user state so that access to the host computer system is limited to physical access at the host computer system.

According to the interpretation proposed by the Office, the system of Mann (i.e., the Internet and the personal computer) corresponds to the host computer system of claim 1, and the system of Mann operates in a multi-user mode by communicating. However, this interpretation fails because the system of Mann cannot perform the method of "taking the host computer system down to a single user state," as recited in claim 1.

While the Office suggests that "isolation of the computer from the Internet results in the computer operating in a single user state," the Office ignores the fact that its proposed system of Mann also includes the Internet, and the Office fails to explain how a system that includes the Internet can be reduced to a single user state. It is improper for the Office to propose a system from the reference to explain one element of the claim and to disregard the proposed system in explaining a second element of the same claim. The system proposed by the Office fails to disclose or suggest each and every element of claim 1.

Additionally, "determination of obviousness cannot be based on the hindsight combination of components selectively culled from the prior art to fit the parameters of the patented invention." ATD Corp. v. Lydall, Inc., 159 F.3d 534, 48 USPQ2d 1321 (Fed. Cir. 1998). In Mann, the data sending device is separate from the data receiving device. *See Mann*, col. 2, line 61 to col. 3, line 5 and Figure 1. Accordingly, it is improper to selectively cull Mann to combine the separate elements for the purpose of explaining the "multi-user mode," and then ignore the fact that Mann teaches isolating the receiving device "without disrupting normal operation." *See Mann*, col. 2, lines 30-32. If a user state of the data receiving device of Mann is

changed by disconnecting the device, as suggested by the Office, then the advantage of Mann is undermined. Accordingly, the asserted combination does not teach or suggest "taking the host computer system down to a single user state," as recited in claim 1.

Further, the interpretation proposed by the Office is technically inconsistent with the teachings of Mann. Mann fails to disclose or suggest that an operating state of the data sending device or of the data receiving device is altered. Instead, Mann discloses that the devices are isolated "without disrupting normal operation of either entity." *See Mann*, col. 2, lines 30-32. In Mann, the state of the operating mode of the sending entity is not altered by the termination of the connection to the Internet. *See Mann*, col. 2, lines 30-32. Instead, the data isolator disconnects the data receiving entity from the data sending entity (i.e., disconnects the personal computer from the Internet). *See Mann*, col. 2, line 62 to col. 3, line 5. Thus, the connection between the data sending device and the data receiving device is altered, but Mann fails to disclose or suggest that a user state of the data receiving device is altered.

Additionally, in Mann, the data isolator is disclosed as operating the same way whether the data receiving device is a personal computer or a local area network. When the data receiving entity is a Local Area Network (as suggested by Mann at col. 2, line 64), the local area network is not indicated to be reduced to a single user state. Consistent with the teachings of Mann, the local area network can be isolated from the Internet, but otherwise continues to operate without disruption to normal operation. *See Mann*, col. 2, line 30-32. Accordingly, Mann fails to disclose or suggest altering a user state associated with either the sending data entity or the receiving data entity.

The suggestion by the Office, at page 7 of the Examiner's Answer, that severing the communication between the Internet and the personal computer "results in the computer operating in a single user state" is unsupported by the reference and should not be sustained. Communications between a first user at a data sending entity and a second user at a data receiving entity does not implicate a user state of the data receiving entity.

Thus, for at least the foregoing reasons, the cited references, including Douglas and Mann, alone or in combination, fail to disclose or suggest each and every element of the claims.

Accordingly, the rejection of claims 1, 3-15 and 17-27 over Douglas and Mann is improper and should be withdrawn.

IV. CONCLUSION

For at least the above reasons, all pending claims are allowable and a notice of allowance is courteously solicited. Please direct any questions or comments to the undersigned attorney at the address indicated. Appellant respectfully requests reconsideration and allowance of all claims and respectfully requests that this patent application be advanced to issue.

Respectfully submitted,

10-4-2007
Date

Jeffrey G. Toler; Reg. No. 38,342
Attorney for Applicant(s)
TOLER SCHAFFER LLP
8500 Bluffstone Cove, Suite A201
Austin, Texas 78759
(512) 327-5515 (phone)
(512) 327-5575 (fax)